UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

NELSON ESTRADA, individually and on behalf of all others similarly situated, Plaintiff, v. TASKUS, INC. Defendant	CASE NO. 1:25-cv-4409 **COMPLAINT – CLASS ACTION** JURY TRIAL DEMANDED

Plaintiff Nelson Estrada ("Plaintiff"), individually and on behalf of all others similarly situated, by and through the undersigned attorneys, brings this class action against Defendant TaskUs, Inc. ("TaskUs") and complains and alleges upon personal knowledge and information and belief as to all other matters:

INTRODUCTION

1. Plaintiff brings this class action against TaskUs, a business process outsourcing ("BPO") company that provides services to Coinbase, Inc. ("Coinbase"), for its failure to secure and safeguard his and millions of other individuals' personally identifiable information, including names, addresses, phone numbers, email addresses, social security numbers, bank account numbers, bank account identifiers, government-ID images, and account data (collectively, "PII"). As a result of their failures, Plaintiff and as many as millions of other individuals whose data has been entrusted to Defendant suffered present injury and damages including identity theft, loss of value of their PII, out-of-pocket expenses, the value of their time reasonably incurred to remedy

or mitigate the effects of the unauthorized access, exfiltration, and subsequent criminal misuse of their sensitive and highly personal information.

2. Defendant TaskUs is a Delaware corporation with its corporate headquarters in New Braunfels, Texas. TaskUs is a BPO, which describes itself as the "outsourcing partner of choice for many of the most disruptive brands in the world."[1] TaskUs provides thousands of outsourced, low-paid employees to perform customer service support for major technology-sector clients.

3. Coinbase utilizes TaskUs to provide outsourced customer service support from personnel located in India.

4. Coinbase is a multinational publicly traded company operating a cryptocurrency exchange that allows investors to buy, sell, and transfer over 250 cryptocurrencies. Founded in 2012, Coinbase is the largest cryptocurrency exchange in the United States regarding trading volume, with over 9.7 million monthly transacting users worldwide, 245,000 ecosystem partners, and reported revenue of $6.3 billion in 2024.

5. On May 14, 2025, Coinbase publicly disclosed that cyber criminals allegedly bribed and recruited a group of allegedly "rogue overseas support agents" to steal Coinbase PII to facilitate social engineering attacks and then tried to extort Coinbase for $20 million to cover up the data theft (the "Data Breach").[2] Coinbase disclosed that a threat actor obtained its customers' PII "by paying multiple contractors or employees working in support roles outside the United States to collect information from internal Coinbase systems..." In subsequent interviews concerning the Data Breach, Coinbase employees disclosed that those contractors or employees

[1] TaskUs, Inc. Form S-1, Registration Statement, at 1, *available at* https://ir.taskus.com/node/6826/ixbrl-viewer.

[2] Form 8-K, Coinbase Global, Inc. (May 14, 2025).

were located in call centers in India. Coinbase publicly disclosed that it estimated customer losses to be within the range of approximately $180 million to $400 million. Coinbase also disclosed that the breach had affected as many as 1% of Coinbase's 9.7 million monthly active customers.[3]

6. Upon information and belief, and as further set forth below, the "rogue overseas support agents" Coinbase identified as having exfiltrated Coinbase customer data worked for Defendant's India-based customer call centers. For example, in early January of 2025, TaskUs reportedly abruptly terminated over 300 employees from its India-based call centers, citing allegations of fraud. At the same time, Bloomberg has reported that Coinbase executives stated that they first became aware of the Data Breach in January of 2025. Coinbase also disclosed to the SEC that upon the discovery of the Data Breach, Coinbase "immediately terminated the personnel involved." The reported timeline of Coinbase's awareness of the Data Breach coincides directly with TaskUs' involvement in the Data Breach. Moreover, those involved in the termination of TaskUs personnel in January 2025 have claimed that those TaskUs personnel were terminated because they committed fraud with respect to their work on Coinbase matters. Nevertheless, TaskUs and Coinbase failed to timely notify Plaintiff and other Class Members. Between January of 2025, when they became aware of the Data Breach and May of 2025, TaskUs disclosed in its Form 10-Ks that they were not aware of any material data breaches impacting their respective companies.

7. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect PII from the foreseeable threat of a cyberattack. By being entrusted with Plaintiff's and Class Members' PII for its own pecuniary benefit, Defendant assumed a duty to Plaintiff and Class Members to

[3] Protecting Our Customers- Standing Up to Extortionists, *Coinbase Blog,* available at https://www.coinbase.com/blog/protecting-our-customers-standing-up-to-extortionists.

implement and maintain reasonable and adequate security measures to secure, protect, and safeguard Plaintiff's and Class Members' PII against unauthorized access and disclosure. Defendant also had a duty to adequately safeguard this PII under applicable law, as well as pursuant to industry standards and duties imposed by statutes, including Section 5 of the Federal Trade Commission Act ("FTC Act").

8. Defendant breached those duties by, among other things, failing to implement and maintain reasonable security procedures and practices to protect the PII in its possession from unauthorized access and disclosure. As a result of Defendant's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiff and up to millions of Class Members suffered injury and ascertainable losses in the form of pecuniary damages from the loss of their crypto assets, out of-pocket expenses, loss of value of their time reasonably incurred to remedy or mitigate the effects of the attack, the diminution in value of their personal information from the exposure, the present and imminent thread of fraud and identity theft, and the pecuniary losses and damages resulting from the Data Breach. This action seeks to remedy these failings and their consequences.

9. Defendant's failure to timely notify the victims of its Data Breach meant that Plaintiff and Class Members were unable to immediately take affirmative measures to prevent or mitigate the resulting harm. Despite having been accessed and exfiltrated by unauthorized criminal actors, Plaintiff's and Class Members' sensitive and confidential PII remains in the possession of TaskUs. Absent additional safeguards and independent review and oversight in the form of injunctive relief, the information remains vulnerable to further cyberattacks and theft.

10. Defendant disregarded the rights of Plaintiff and Class Members by, inter alia, failing to take adequate and reasonable measures to ensure its data systems were protected against

unauthorized intrusions; failing to implement adequately robust computer systems and security practices to safeguard PII; failing to take standard and reasonably available steps to prevent the Data Breach; failing to adequately train and oversee its staff and employees on proper security measures; and failing to provide Plaintiff and Class Members with prompt and adequate notice of the Data Breach.

11. In addition, Defendant failed to properly monitor the computer network and systems that housed the PII. Had Defendant properly monitored these electronic systems, it would have discovered the intrusion sooner or prevented it altogether. The security of Plaintiff's and Class Members' identities is now at risk because of Defendant's wrongful conduct, as the PII that Defendant collected and maintained is now in the hands of data thieves. This present harm will continue for the course of their lives.

12. Armed with the PII accessed in the Data Breach, data thieves can commit a wide range of crimes including, for example, converting Plaintiffs' cryptocurrency assets, opening new financial accounts in Class Members' names, taking out loans in their names, using their identities to obtain government benefits, filing fraudulent tax returns using their information, obtaining driver's licenses in Class Members' names, and giving false information to police during an arrest. Data thieves and criminals can also use Plaintiff and Class Members' addresses to initiate physical attacks in order to steal their cryptocurrency assets. In fact, public reporting indicates that many Coinbase customers have invested in bodyguards to deter kidnappers following the Data Breach.

13. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a present and imminent risk of fraud, identity theft, and physical attacks. Coinbase has estimated that losses as a result of stolen cryptocurrency assets from the Data Breach may be as high as $400 million to date. Other public reports indicate that the Data Breach may subject Class Members to

physical harms from criminals using PII including Class Members' personal address in order to steal their cryptocurrency assets. Among other measures, Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft. Further, Plaintiff and Class Members will incur out-of-pocket costs to purchase adequate credit monitoring and identity theft protection and insurance services, credit freezes, credit reports, or other protective measures to deter and detect identity theft. Plaintiff and Class Members will also be forced to expend additional time to review credit reports and monitor their financial accounts for fraud or identity theft. Moreover, because the exposed information includes Social Security numbers (or portions of those numbers) and other immutable personal details, the risk of identity theft and fraud will persist throughout their lives.

14. Plaintiff and Class Members seek to hold TaskUs responsible for the harms resulting from the massive and preventable disclosure of such sensitive and personal information. Plaintiff seeks to remedy the harms resulting from the Data Breach on behalf of himself and all similarly situated individuals whose PII was accessed and exfiltrated during the Data Breach. Plaintiff, individually and on behalf of all other Class Members, brings claims for negligence, negligence per se, breach of implied contract, unjust enrichment, breach of confidence, for declaratory and injunctive relief, violation of the Unfair Business Practices statutes of various states, and Violation of the California Consumer Privacy Act. To remedy these violations of law, Plaintiff and Class Members seek actual damages, statutory damages, restitution, and injunctive and declaratory relief (including significant improvements to Defendant's data security protocols and employee training practices); reasonable attorneys' fees, costs, and expenses incurred in bringing this action; and all other remedies the Court deems just and proper.

PARTIES

Plaintiff

15. Plaintiff Nelson Estrada resides in Miami, Florida. He maintains an account with Coinbase in which he stores cryptocurrency assets. On May 15, 2025, he received a notice from Coinbase stating that individuals providing "overseas support" services "improperly accessed information related to [Mr. Estrada's] account."

Defendant

16. Defendant TaskUs, Inc. is a Delaware corporation with its principal place of business in Texas. TaskUs had access to Coinbase customers' PII and failed to secure the received PII or implement appropriate security measures or screening procedures to ensure that its agents, support representatives, and other individuals to whom Plaintiff and Coinbase entrusted the PII data would ensure secure handling of the data.

JURISDICTION AND VENUE

17. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

18. This Court has personal jurisdiction over TaskUs because TaskUs conducts substantial business in New York and in this District; engaged in the conduct at issue herein from and within this District, including by collecting and storing PII provided by Class Members to Coinbase, a company based in and headquartered in New York; and otherwise has substantial contacts with this District and purposely availed itself of the Courts in this District, including by collecting and then compromising PII of a substantial number of New York residents.

19. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(2) because this District is where a substantial part of the acts, omissions, and events giving rise to Plaintiff's claims occurred. Specifically, TaskUs acquired Coinbase PII through its relationship with Coinbase, which is based in New York, New York. TaskUs regularly conducts business in New York related to Coinbase and a substantial number of Coinbase customers reside in New York, New York, and thus suffered damages here as a result of the Data Breach.

I. The Data Breach

20. On May 14, 2025, Coinbase announced that an unnamed threat actor claimed to have obtained Coinbase customers' PII including their names, addresses, phone numbers, email addresses, portions of their social security numbers, account information, bank account information, governmental-ID images, and account data. TaskUs did not make a similar disclosures even though it was involved in the Data Breach. In a blog post, Coinbase stated that "[c]yber criminals bribed and recruited a group of rogue overseas support agents to steal Coinbase data to facilitate social engineering attacks. These insiders abused their access to customer support systems to steal the account data for a small subset of customers."[4] Coinbase stated that the attackers demanded $20 million to cover up the attack, but that Coinbase refused to pay the ransom.

21. Coinbase customers have claimed, in the months leading up to Coinbase's May 14, 2025 disclosure, that individuals posing as Coinbase customer support teams requested their Coinbase wallet passwords and two-factor identification ("2FA") in an attempt to exfiltrate the contents (and value) of their Coinbase wallets. These customers have claimed that individuals contacted Coinbase customers posing as Coinbase customer support personnel

[4] Protecting Our Customers- Standing Up to Extortionists, *Coinbase Blog,* available at https://www.coinbase.com/blog/protecting-our-customers-standing-up-to-extortionists.

by relaying to the Coinbase customers data that could have only been in the possession of Coinbase or their outsourced BPOs, including TaskUs. That information included balances, transaction history, customer addresses, and other information. Some Coinbase customers then provided the criminals posing as Coinbase employees with their 2FA, resulting in the theft of the cryptocurrency held in their Coinbase wallets. Coinbase estimates that as much as $400 million has been stolen from customers using data exfiltrated in the Data Breach to date.

22. Between April 23, 2025 and May 25, 2025, Plaintiff Estrada received nine separate communications purporting to come from Coinbase indicating that Plaintiff had attempted to login and providing a false number for Mr. Estrada to contact support.

23. Upon information and belief, the group of allegedly "rogue overseas support agents" responsible for the Data Breach are employees of TaskUs.

24. TaskUs provides overseas customer support services for Coinbase. TaskUs, for example, publicizes in its SEC filings that it works with Coinbase. Coinbase executives have also appeared at TaskUs events to describe how Coinbase utilizes TaskUs. And several TaskUs employees, including employees based in India, describe their work at TaskUs as encompassing customer support functions for Coinbase.

25. Through their work for Coinbase, TaskUs employees have access to a variety of customer information, including, but not limited to the PII at issue in the Data Breach.

26. In January 2025, TaskUs abruptly terminated 300 employees from their Indore, India-based call center, citing allegations of fraud.[5] Those terminations coincided with the time in which Coinbase allegedly first became aware of the wrongdoing that ultimately led to the Data

[5] Financial Express, *TaskUs, Indore based BPO Fires Over 300 Employees Without Notice, Sparks Staff Protests,* Jan. 11, 2025, *available at https://www.financialexpress.com/business/industry/taskus-indore-based-bpo-fires-over-300-employees-without-notice-sparks-staff-protests/3712402/.*

Breach. Those involved in the terminations have stated that the fraud pertained to TaskUs' provision of support services to Coinbase. At least one Indore, India-based TaskUs employee who reportedly worked for Coinbase's customer support abruptly ended her employment with TaskUs in January of 2025, the same time that TaskUs terminated 300 employees for alleged fraud.

27. Neither Coinbase nor TaskUs disclosed the basis for the termination of those 300 employees in January of 2025. In fact, TaskUs' Form 10-K, filed with the SEC in February 2025, stated that it was not aware of any material data breach impacting the company. Less than one week before Coinbase publicly disclosed the Data Breach to its customers, Blackstone, along with TaskUs' co-founders, executed a buy-out to take TaskUs private.

28. TaskUs and Coinbase were aware of the Data Breach as early as January of 2025, if not earlier, but did not notify Coinbase customers until Coinbase's May 14, 2025 disclosure. In an interview with Bloomberg News, Coinbase personnel acknowledged that the company began noticing unusual activity from its customer representatives as far back as January, the same time that TaskUs terminated 300 employees at its Indore, India call center.[6]

29. The May 14, 2025 disclosure by Coinbase was flawed and misleading. Namely, neither Coinbase nor TaskUs immediately warned affected customers and instead waited until the Defendant's employees threatened to expose the Data Breach unless Coinbase paid a $20 million ransom. Plaintiff and Class Members are still completely in the dark about the extent of the breach as well.

30. The PII contained in the files accessed by cybercriminals appears not to have been encrypted because if properly encrypted, the attackers would have acquired unintelligible data

[6] Bloomberg, *Coinbase Hack Rocks Company That Led Crypto Into Mainstream*, May 15, 2025, *available at* https://www.bloomberg.com/news/articles/2025-05-15/coinbase-says-bribed-workers-leaked-data-to-hacker-seeking-20-million-in-ransom.

and would not have accessed Plaintiff's and Class Members' PII.

31. The Data Breach reportedly impacted the PII of nearly 1% of Coinbase's monthly active users. Upon information and belief, Coinbase's disclosure of the number of customers affected by the Data Breach vastly underestimates the number of customers impacted by the Data Breach. In particular, numerous customers, including many who have not received a notification regarding the Data Breach from Coinbase, have inundated public message boards to complain that they have received outreach from individuals posing as Coinbase customer support.

32. Meanwhile, Binance and Kraken, two other cryptocurrency exchanges that compete with Coinbase, were reportedly able to avoid the same social engineering hacks at issue in the Coinbase Data Breach. In particular, while scammers reportedly reached out to Binance customer-service agents with bribery offers, Binance or its outsourced BPOs utilized artificial intelligence bots to prevent fraud. Upon information and belief, TaskUs did not use similar tools to prevent fraud, nor did they employ other reasonably available and necessary preventative measures.

II. TaskUs Failed to Follow FTC Guidelines and Industry Standards

33. Federal and state regulators have established security standards and issued recommendations to prevent data breaches and the resulting harm to consumers and employees. There are a number of state and federal laws, requirements, and industry standards governing the protection of Private Information. For example, at least 24 states have enacted laws addressing data security practices that require businesses that own, license, or maintain Private Information about a resident of that state to implement and maintain "reasonable security procedures and practices" and to protect Private Information from unauthorized access.

34. Defendant is also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

35. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

36. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.

37. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

38. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

39. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

40. The FTC has brought enforcement actions against businesses, including third-party vendors, for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

41. In 2023, the FTC issued another guide for businesses, entitled *Start with Security: Lessons Learned from FTC Cases.* In that review of decades of FTC enforcement actions against businesses, the FTC warned companies not to collect personal information that they do not need, to restrict access to sensitive data, to limit administrative access, to require secure passwords and authentication, to store sensitive personal information securely and protect it during transmission, to segment a business' network and monitor those trying to access data, and to secure remote access to a business' network. Notably, the FTC also warned companies to "keep a watchful eye on your service providers" and monitor them for compliance with reasonable security measures.

42. At all times, Defendant failed to properly implement some or all of these (and other) basic data security practices.

43. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to individuals' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

44. Defendant was at all times fully aware of their obligation to protect Coinbase's customers' PII. TaskUs's 2024 10-K, for example, states that "[b]ecause we have access to our clients' sensitive and confidential information in the ordinary course of our business, our

employees have engaged and could engage in criminal, fraudulent, or other conduct prohibited by applicable law, client contracts or internal policy."

45. TaskUs has a history of failing to implement appropriate security measures to protect against fraudulent activities by its employees. Its 2024 10-K securities failing acknowledges that: "it is possible that our security controls and practices may not prevent unauthorized or other improper access to our technology, infrastructure, data, equipment, or systems, or the disclosure or misuse of personal, protected health or proprietary information." In 2022, cryptocurrency investors filed a class action complaint against TaskUs related to a similar data breach in which "certain 'rogue' TaskUs employees took advantage of [third-party] customer information" to leak customer information similar to the PII at issue here.[7] According to the complaint, customers lost money in phishing attacks and faced threats of physical violence or blackmail if they did not transfer crypto-assets to criminals around the world.

46. Experts routinely identify customer service providers as being particularly vulnerable to cyberattacks because of the value of the PII that these entities collect and maintain.

47. Several best practices have been identified that at a minimum should be implemented by corporate entities like TaskUs, including, but not limited to: educating all employees about cybersecurity; requiring strong passwords; maintaining multi-layer security, such as firewalls and anti-virus and anti-malware software; utilizing encryption (e.g., making data unreadable without a key); utilizing multi-factor authentication; backing up data; and limiting the number of employees with access to sensitive data.

[7] *Forsberg* v. *Shopify, Inc. et al.*, C.A. No. 22-cv-346 (D. Del. Apr. 1, 2022).

48. Other standard best cybersecurity practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

49. Defendant failed to meet the minimum standards of, e.g., the NIST Cybersecurity Framework, and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established industry standards in reasonable cybersecurity readiness.

50. These foregoing frameworks are existing and applicable industry standards in the corporate sector and Defendant failed to comply with these accepted standards, thereby opening the door to cybercriminals and causing the Data Breach.

51. Defendant's wrongful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber attacks;

b. Failing to heed data security warnings and implement appropriate steps to mitigate the risks related to such warnings;

c. Failing to adequately protect current or former customers' PII;

d. Failing to implement updates and patches in a timely manner;

e. Failing to properly monitor data security systems for existing intrusions, exfiltration of data, brute force attempts, and clearing of event logs;

f. Failing to adequately supervise staff handling PII;

g. Failing to ensure that all employees and third-partyes apply all available

and necessary security updates;

h. Failing to ensure that all employees and third parties practice the principle of least privilege and maintain credential hygiene; and failing to avoid the use of domain wide, admin-level service accounts;

III. TaskUs Owed Plaintiff and Class Members a Duty to Safeguard Their PII

52. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII of Plaintiff and Class Members.

53. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the PII in its possession, including adequately training its employees and others who accessed PII within its computer systems on how to adequately protect PII and adequately supervising its employees to ensure that those who accessed PII did so with an adequate business purpose.

54. Defendant owed a duty to Plaintiff and Class Members to implement processes that would detect a compromise of PII in a timely manner.

55. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

56. Defendant owed a duty to Plaintiff and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

57. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of inadequate data security practices.

IV. TaskUs Knew That Criminals Target PII

58. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in industries holding significant amounts of PII preceding the date of the breach.

59. At all relevant times, Defendant knew, or should have known, that Plaintiff's and all other Class Members' PII was a target for malicious actors. Despite such knowledge, Defendant failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class Members' PII from cyberattacks that Defendant should have anticipated and guarded against.

60. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the PII belonging to Coinbase's customers like Plaintiff and Class Members.

61. PII is a valuable property right. The value of PII as a commodity is measurable. "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[8] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[9] Personal data is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web,"

[8] OECD (2013), "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value", OECD Digital Economy Papers, No. 220, OECD Publishing. http://dx.doi.org/10.1787/5k486qtxldmq-en

[9] U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017, Interactive Advertising Bureau (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

for many years.

62. As a result of its real value and the recent large-scale data breaches, identity thieves and cybercriminals have openly posted credit card numbers, Social Security numbers, PII, and other sensitive information directly on various websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

63. Personally identifiable information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200 on the black market to thieves who desire to extort and harass victims, and to take over victims' identities.[10]

64. Criminals can use stolen PII to extort a financial payment through social engineering attacks. For example, armed with just a name and date of birth, a data thief can solicit additional information from a victim regarding their identity, such as a person's login credentials or full social security number.

65. The Data Breach was especially harmful because it exposed non-public details of users' cryptocurrency accounts – balances, wallet addresses, and recent transaction history. Possessing that insider information, the attackers could plausibly pose as Exchange personnel and use various social-engineering tactics to gain control of victims' accounts or divert their assets elsewhere. Consequently, the stolen data commands a high black-market price and enables ongoing schemes that put Plaintiffs and the Class at serious risk of further financial loss.

66. Consumers place a high value on the privacy of that data. According to the

[10] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

Government Accountability Office, "law enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft . . . . As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harms."[11]

V. *Theft of PII has Grave and Lasting Consequences for Victims*

67. Theft of PII is serious. The FTC warns consumers that identity thieves use PII to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[12]

68. Identity thieves use PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan, change a billing address so the victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card number to withdraw funds, obtain a new driver's license or other form of identification, and/or use the victim's information in the event of arrest or court action.[13]

69. With access to an individual's PII, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture, using the victim's name and Social Security number to obtain government benefits, or filing a

[11] GAO Report at 29.
[12] *See What to Know About Identity Theft*, Federal Trade Commission Consumer Advice, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed on Jan. 25, 2024).
[13] Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, Experian (Sept. 1, 2017), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.

70. Each year, identity theft causes billions of dollars of losses to victims in the United States. For example, with the PII stolen in the Data Breach, which includes Social Security numbers, identity thieves can open financial accounts, commit medical fraud, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft. These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class Members.

71. Personally identifiable information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use the information and trade it on dark web black-markets for years to come.

72. For example, it is believed that certain highly sensitive personal information compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related unemployment benefits.

73. The PII exposed in this Data Breach is valuable to identity thieves for use in the kinds of criminal activity described herein. These risks are both certainly impending and substantial. As the FTC has reported, if cyberthieves get access to a person's highly sensitive information, they will use it.

74. Identity thieves can use Social Security numbers to obtain a driver's license or

official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

75. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.

76. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. Fraud and identity theft resulting from the Data Breach may go undetected until criminals attempt to utilize such PII in social engineering hacks months, or even years, later. An individual may not know that her or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

77. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.

78. Victims of the Data Breach, like Plaintiff and Class Members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.

79. As a direct and proximate result of the Data Breach, Plaintiff and Class Members

have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff and Class Members must now m the time and expend the effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and other account information for unauthorized activity for years to come.

80. Plaintiff and Class Members have suffered or will suffer actual harms for which they are entitled to compensation, including, but not limited to the following:

a. Trespass, damage to, and theft of their personal property, including PII;

b. Improper disclosure of their PII;

c. The imminent and certainly impending injury flowing from actual and potential future fraud and identity theft posed by their PII being in the hands of criminals and having already been misused;

d. The imminent and certainly impending risk of having their confidential PII used against them by spam callers to defraud them;

e. Damages flowing from Defendant's untimely and inadequate notification of the Data Breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

h. Ascertainable losses in the form of deprivation of the value of Plaintiff's and Class Members' PII for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their PII; and

k. Increased cost of borrowing, insurance, deposits, and other items which are adversely affected by a reduced credit score.

81. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which remains in the possession of Defendan, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. Defendant has shown to be incapable of protecting Plaintiff's and Class Members' PII.

VI. *The Data Breach was Foreseeable and Preventable*

82. Given prior accusation that allegedly rogue TaskUs employees compromised customer PII in a similar attack against Shopify, the Data Breach at issue here was both foreseeable and preventable. Defendant's securities filings disclose the potential of unauthorized access, including intentional misconduct or other malfeasance by Defendant's employees. As explained by the FBI, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."

83. Plaintiff and Class Members entrusted their PII to Coinbase, and thus to Defendant with a reasonable expectation and mutual understanding that Defendant would comply with their obligations to keep such information confidential and secure from unauthorized access.

84. Plaintiff and Class Members understood and expected that Defendant or anyone in Defendant's position would safeguard their PII against cyberattacks, delete or destroy PII that Defendant was no longer required to maintain, and timely and accurately notify them if their PII was compromised.

VII. *Damages Sustained by Plaintiff and Class Members*

85. Plaintiff and Class Members have been damaged by the compromise of their PII in the Data Breach.

86. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have Plaintiffs suffered actual injury from having their PII compromised as a result of the Data Breach including, but not limited to (a) misuse of their compromised PII; (b) damage to and diminution in the value of their PII, a form of property that Defendant obtained from Plaintiffs; (c) violation of their privacy, including the compromise of highly sensitive PII; (d) present, imminent and impending injury arising from the increased risk of identity theft and fraud; and (e) actual and potential out-of-pocket losses including the loss of time.

87. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class Members.

88. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring financial and other sensitive accounts and

finding fraudulent transfers, insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions and/or government agencies to dispute unauthorized and fraudulent activity in their names;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security numbers, insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

g. Enhancing the privacy and on-chain anonymity of self-custodied cryptocurrency holdings—e.g., rotating wallet addresses, generating new seed phrases, acquiring additional hardware wallets, and employing privacy-preserving tools—incurring both equipment costs and significant personal time;

h. Migrating digital-asset balances to more secure custodial or multi-signature solutions that advertise protections against cyber and physical, and paying the associated account-setup fees, transfer fees, and ongoing service charges;

89. Plaintiff and Class Members suffered actual injury from having their PII compromised as a result of the Data Breach including, but not limited to: (a) damages and out-of pocket losses from the misuse of their compromised PII; (b) damage to and diminution in the value of their PII, a form of property that Defendant obtained from Plaintiff and Class Members; (c) violation of their privacy rights; (d) imminent and impending injury arising from the increased risk of identity theft and fraud; and (e) emotional distress.

90. Defendant disregarded the rights of Plaintiff and Class Members by, *inter alia*,

(i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that their PII was protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class Members' PII; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class Members with prompt and accurate notice of the Data Breach.

CLASS ALLEGATIONS

91. Plaintiff brings this class action individually and on behalf of all members of the following class of similarly situated persons pursuant to Federal Rule of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4):

> Nationwide Class
>
> All persons in the United States whose PII was compromised in the Data Breach.

92. Plaintiff proposes the following Subclass definition, subject to amendment as appropriate:

> California Subclass
>
> All persons in the State of California whose PII was compromised in the Data Breach.

93. Excluded from the Classes are Defendant and Defendant's subsidiaries, affiliates, officers, directors, and any entity in which Defendant has a controlling interest; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

94. Plaintiffs reserve the right to modify or amend the definition of the proposed

Class before the Court determines whether certification is appropriate.

95. Numerosity: The members in the Class are so numerous that joinder of all Class Members in a single proceeding would be impracticable. Coinbase disclosed that at least 97,000 individuals' PII has been compromised.

96. Commonality and Predominance: Common questions of law and fact exist as to all Class Members and predominate over any potential questions affecting only individual Class Members. Such common questions of law or fact include, *inter alia*:

a. Whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class Members' PII from unauthorized access and disclosure;

b. Whether the computer systems and data security practices employed by Defendant to protect Plaintiff's and Class Members' PII violated the FTC Act, and/or state laws and/or Defendant's other duties discussed herein;

c. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and Class Members;

d. Whether Plaintiff and Class Members suffered injury as a proximate result of Defendant's negligent actions or failures to act;

e. Whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiff's and Class Members' PII;

f. Whether an implied contract existed between Class Members and Defendant providing that Defendant would implement and maintain reasonable security measures to protect and secure Class Members' PII from unauthorized access and disclosure;

g. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiff and Class Members;

h. Whether Defendant's actions and inactions alleged herein constitute gross negligence;

i. Whether Defendant breached its duties to protect Plaintiff's and Class Members' PII; and

j. Whether Plaintiff and all other members of the Class are entitled to damages and the measure of such damages and relief.

97. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of all other Class Members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

98. Typicality: Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had PII compromised in the Data Breach. Plaintiff and Class Members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class Members.

99. Adequacy: Plaintiff will fairly and adequately protect the interests of the Class

Members. Plaintiff is an adequate representative of the Class and has no interests adverse to, or in conflict with, the Class that Plaintiff seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

100. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action.

101. Adequate notice can be given to Class members directly using information maintained by Defendants or by Coinbase.

102. **Predominance**. The issues in this action are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Defendant has engaged in a common course of conduct toward Plaintiffs and Class members. The common issues arising from Defendant's conduct affecting Class members set out above predominate over any individualized issues. Adjudication of these issues in a single action has important and desirable advantages of judicial economy.

COUNT I: NEGLIGENCE

103. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

104. Defendant owed a duty to Plaintiff and all other Class Members to exercise reasonable care in safeguarding and protecting their PII in its possession, custody, or control.

105. Defendant knew, or should have known, the risks of collecting and storing Plaintiff's and Class Members' PII and the importance of maintaining secure systems.

Defendant knew, or should have known, of the many data breaches that targeted companies holding significant amounts of PII in recent years.

106. Given the nature of Defendant's business, the sensitivity and value of the PII it maintains, and the resources at its disposal, Defendant should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

107. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to it—including Plaintiff's and Class Members' PII. Defendant also breached these duties by failing to supervise and oversee their employees, including by implementing appropriate technology to monitor and audit their employees' access to and use of PII.

108. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class Members' PII to unauthorized individuals.

109. But for Defendant's negligent conduct or breach of the above-described duties owed to Plaintiff and Class Members, their PII would not have been compromised.

110. As a result of Defendant's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other

Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) actual or attempted fraud.

COUNT II: NEGLIGENCE PER SE

111. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

112. Defendant's duties arise from, *inter alia*, Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to employ reasonable measures to protect and secure PII.

113. Plaintiff and Class Members are within the class of persons that Section 5 of the FTCA was intended to protect.

114. The harm occurring as a result of the Data Breach is the type of harm that Section 5 of the FTCA intended to guard against.

115. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems,

would result in the release, disclosure, and dissemination of Plaintiff's and Class Members' PII to unauthorized individuals.

116. The injury and harm that Plaintiff and the other Class Members suffered was the direct and proximate result of Defendant's violations of Section 5 of the FTCA. Plaintiff and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vi) actual or attempted fraud.

COUNT III: BREACH OF IMPLIED CONTRACT

117. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

118. Defendant required Plaintiff and Class Members to provide, or authorize the transfer of, their PII in order for Defendant to provide services. In exchange, Defendant entered into implied contracts with Plaintiff and Class Members in which Defendant agreed to comply with its statutory and common law duties to protect Plaintiff's and Class Members' PII and to timely notify them in the event of a data breach.

119. Plaintiff and Class Members would not have provided their PII to Defendant, or would not have agreed to have that information provided to Defendant, had they known that Defendant would not safeguard their PII, as promised, or provide timely notice of a data breach.

120. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendant.

121. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class Members' PII and by failing to provide them with timely and accurate notice of the Data Breach.

122. The losses and damages Plaintiff and Class Members sustained (as described above) were the direct and proximate result of Defendant's breach of its implied contracts with Plaintiff and Class Members.

COUNT IV: UNJUST ENRICHMENT

123. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

124. This claim is pleaded in the alternative pursuant to Fed. R. Civ. P. 8(d).

125. Plaintiff and Class Members conferred a monetary benefit upon TaskUs in the form of monies paid by Coinbase for customer support services and in the form of providing them with PII.

126. Defendant accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Defendant also benefitted from the receipt of Plaintiff's and Class Members' PII.

127. As a result of Defendant's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between Coinbase's payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

128. Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendant failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class Members paid for and that were otherwise mandated by federal, state, and local laws, and industry standards.

129. Defendant should be compelled to provide for the benefit of Plaintiff and Class Members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT V: DECLARATORY AND INJUNCTIVE RELIEF

130. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

131. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

132. Defendant owes a duty of care to Plaintiff and Class Members that require it to adequately secure Plaintiff's and Class Members' PII.

133. Defendant still possesses the PII of Plaintiff and Class Members.

134. Defendant has not satisfied their obligations and legal duties to Plaintiff and Class Members.

135. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their PII and Defendant's failure to address the security failings that led to such exposure.

136. There is no reason to believe that Defendant's employee training and security measures are any more adequate now than they were before the breach to meet Defendant's

contractual obligations and legal duties.

137. Plaintiff, therefore, seeks a declaration (1) that Defendant's existing data security measures do not comply with its duties of care to provide adequate data security, and (2) that to comply with its duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendant engage internal security personnel to conduct testing, including audits on Defendant's systems, on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engages third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audits, tests, and trains its security personnel and employees regarding any new or modified data security policies and procedures;

d. Ordering that Defendant purges, deletes, and destroys, in a reasonably secure manner, any PII not necessary for its provision of services;

e. Ordering that Defendant conducts regular database scanning and security checks; and

f. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information

COUNT VI: VIOLATION OF UNFAIR COMPETITION LAW

138. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein.

139. The laws of all 50 states prohibit unfair competition and provides, in pertinent part, that "unfair competition shall mean and include unlawful, unfair or fraudulent business practices and unfair, deceptive, untrue or misleading advertising." *See e.g.* California Business & Professions Code, sections 17200, et seq ("UCL")

140. Defendant engaged in and continues to engage in "unlawful" business acts and practices under the Unfair Competition Law because Defendant took, accessed, intercepted, tracked, collected, or used the Plaintiffs' and Class Members PII or otherwise failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to it—including Plaintiff's and Class Members' PII. Defendant also breached these duties by failing to supervise and oversee their employees, including by implementing appropriate technology to monitor and audit their employees' access to and use of PII.

141. Defendant has engaged in "unlawful" business practices by violating multiple laws, including California's Customer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), the FTC Act, 15 U.S.C. § 45, and common law.

142. Defendant's conduct as alleged herein was unfair within the meaning of the UCL. The unfair prong of the UCL prohibits unfair business practices that either offend an established

public policy or that are immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers. Defendant failed to implement and maintain reasonable security measures to protect Plaintiffs' and Class Members PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach. Defendant failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security despite knowing the risk of cybersecurity incidents. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiffs and Class Members, whose PII has been compromised.

143. Defendant's conduct violates Section 5 of the Federal Trade Commission Act ("FTCA"), Unfair Competition Law in all 50 states, the California Consumer Privacy Act, Cal. Civ. Code § 1798.150, and California's Consumer Records Act, Cal. Civ. Code § 1798.81.5

COUNT VII: VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT (CCPA) Cal. Civ. Code § 1798.150

(On behalf of California Subclass)

144. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

145. The CCPA, Cal. Civ. Code § 1798.150(a), creates a private cause of action for violations of the CCPA. Section 1798.150(a) specifically provides.

> Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:
>
> (A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

146. Defendant is businesses under § 1798.140(b) in that it is a corporation organized for profit or financial benefit of its shareholders or other owners.

147. Subclass Members are covered "consumers" under subdivision (g) of § 1798.140 in that they are natural persons who are California residents.

148. The personal information of Plaintiff and Subclass Members at issue in this lawsuit constitutes "personal information" under subdivision (a) of § 1798.150 and § 1798.81.5, in that the personal information Defendant collects and which was impacted by the cybersecurity attack includes an individual's including names, addresses, phone numbers, email addresses, social security numbers, bank account numbers, bank account identifiers, government-ID images, and account data.

149. Defendant should have known that their employees engaged in or participated in the Data Breach without Plaintiffs' consent.

150. Defendant subjected Plaintiff's and the Subclass Members' nonencrypted and nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure as a result of the Defendant Rite Aid's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein. repeat the allegations contained in the foregoing paragraphs as if fully set forth herein.

151. As a direct and proximate result of Defendant's conduct, Plaintiff and the Subclass Members were injured and lost money or property, including but not limited to their cryptocurrency assets, the loss of their legally protected interest in the confidentiality and privacy of their personal information, stress, fear, and anxiety, nominal damages, and additional losses

described above.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in their favor and against Defendant as follows:

A. Certifying the Class as requested herein, designating Plaintiff as class representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, individually and on behalf of the Class, seeks appropriate injunctive relief designed to prevent Defendant from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend credit monitoring services and similar services to protect against all types of identity theft.

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

152. Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: May 27, 2025

Respectfully Submitted,

/*Carter E. Greenbaum*

Carter E. Greenbaum
GREENBAUM LAW GROUP, LLP
3 Columbus Circle, Suite 1500
New York, New York 10019
Tel: 212-732-6837
Email: cgreenbaum@greenbaumlawgroup.com